iPhone Security Best Practices

Real-world deployment considerations

Session 625

These are confidential sessions—please refrain from streaming, blogging, or taking pictures.

iPhone Security Best Practices

Shawn Geddis
Enterprise Security Consulting Engineer

Introduction

- Review challenges enterprise IT face with mobile devices
- Expose IT to Security Best Practices for the iPhone
- Discuss iPhone System Integrity
- Explore security enhancements in iPhone OS

What You'll Learn

- The iPhone's built-in security features
- What it means to maintain system integrity
- Intro to tools and methods for deploying organizational policies

iPhone in Enterprise Profiles

Gannett
Media Giant Goes Mobile

Sonnenschein Nath & Rosenthal LLP
Serving Up Innovation

Doylestown Hospital
Always on Call: iPhone 3G

Trek Bikes
iPhone Revolutionizes Bike Sales and Training

Kraft Foods
Serving Up Innovation

YOUR Organization
Your Innovative Use of iPhone

http://www.apple.com/iphone/enterprise/

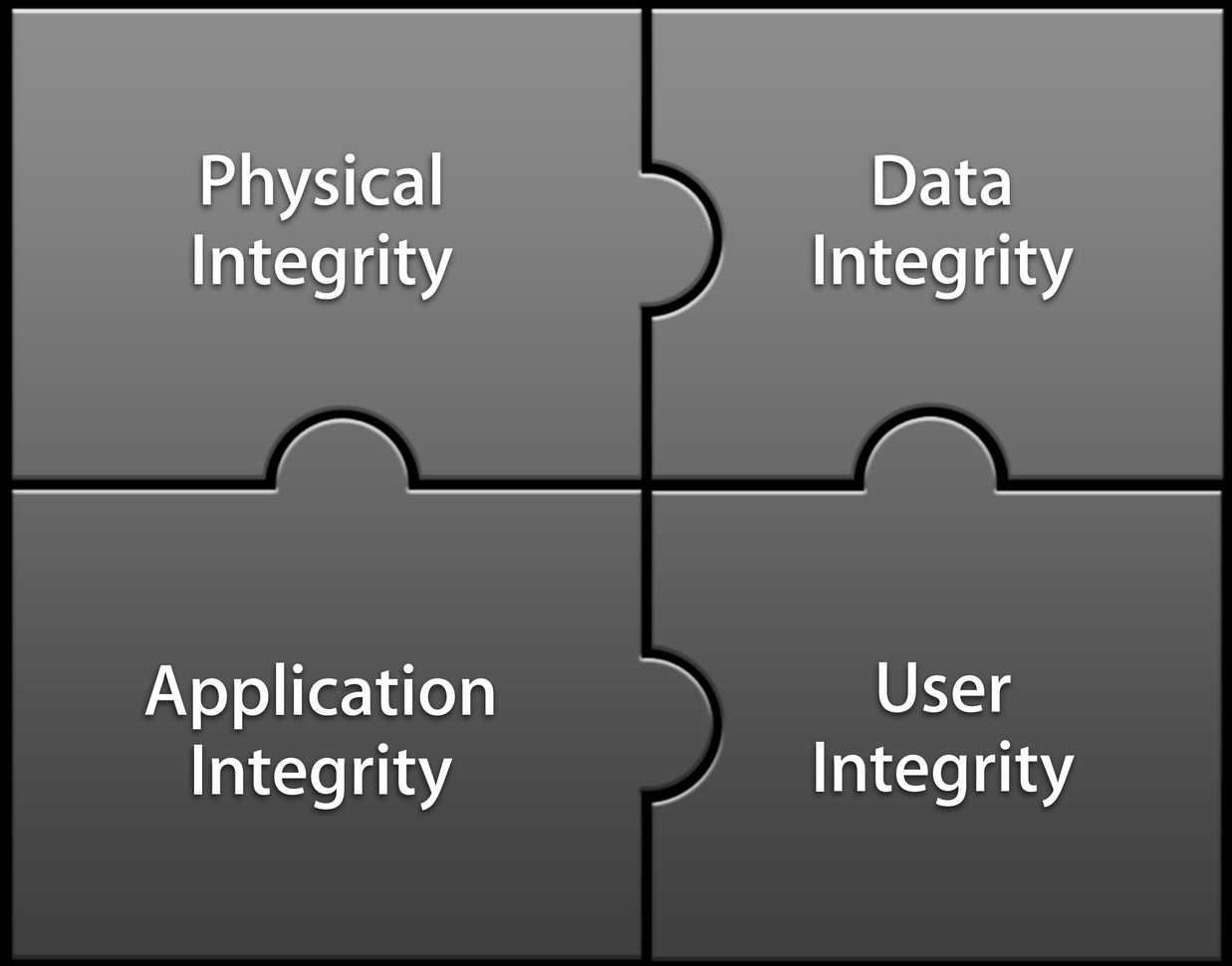
IT Challenges for Mobile Devices

Ensure your *in-house* information stays in-house

System Integrity

“Protecting from unauthorized access, use, disclosure, disruption, modification, or destruction.”

System Integrity



Risk Management

"Identification, assessment, and prioritization of risks followed by coordinated actions to mitigate unfortunate events."

Risks with Mobile Devices

What is there to be worried about?

- Loss or theft of the mobile device
  - Physical access allows for all forms of attacks/compromise
- Access to highly sensitive corporate or personal data
  - Forensic analysis of data stored, Wi-Fi/Bluetooth, audio, …
- Application weaknesses—malicious or accidental
  - Do you know what the application is doing or exposing

Mitigation Measures

Three approaches to reduce potential risk

- "Deny" use of the mobile device or service altogether
  - Can be viewed by user as **Draconian**, so out for now, right?

- "Hope" the user knows what they are doing themselves
  - Heart rate and anxiety level just shot up in the room

- "Enforce" organizational policies on the mobile device
  - A workable solution that all can live with

IT Policy Enforcement Concerns

Ensuring device adheres to IT mandates

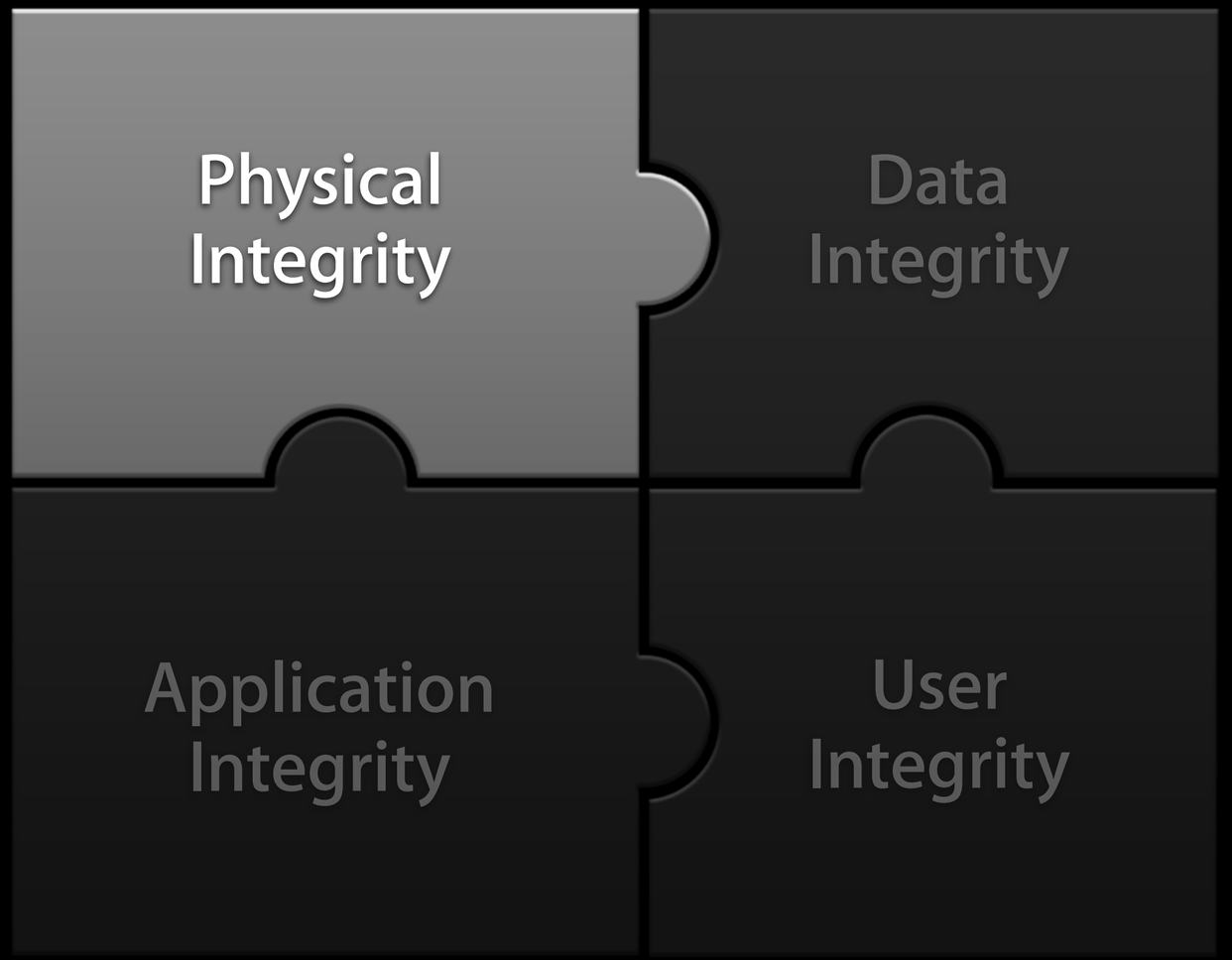
- What are your IT policies on mobile device use
  - Know what it is you are trying to protect from and why

- What are the built-in security features you need to manage
  - How do you configure the device to meet those IT policies

- How do you manage the policies for your iPhone devices
  - Going from **Factory Fresh** to **Corporate Compliant**

Maintaining Integrity

A closer look at integrity



iPhone Configuration Utility 2.0

New and enhanced security policy settings

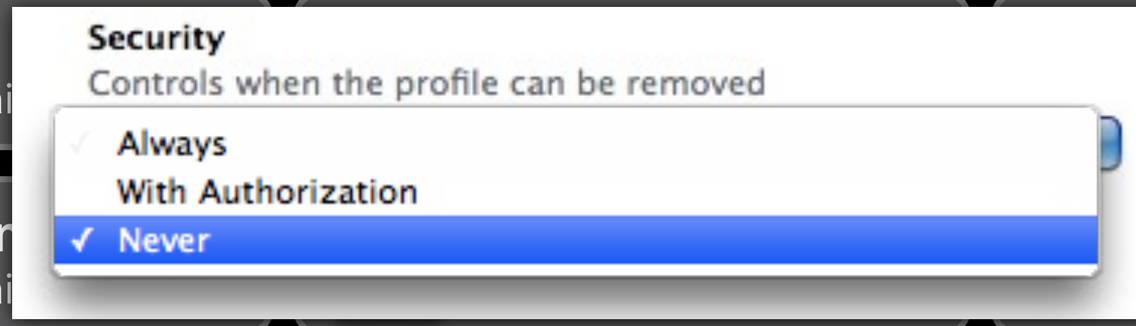
General
Payload Detail Information

Email
Payload Detail Information

Web Clips
Payload Detail Information

Passcode
Payload Detai

Restriction
Payload Detai



Credentials
Payload Detail Information

SCEP
Payload Detail Information

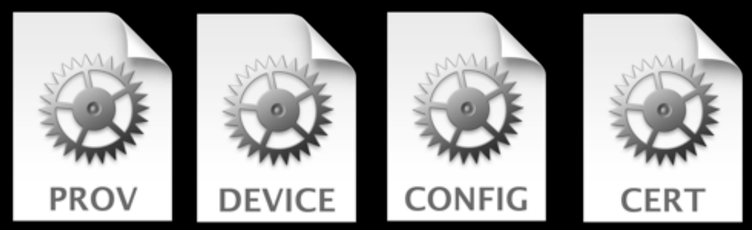
Wi-Fi
Payload Detail Information

CalDAV
Payload Detail Information

Advanced
Payload Detail Information

VPN
Payload Detail Information

Subscribed Calendars
Payload Detail Information



Physical Integrity

Ensuring protection of mobile hardware devices

Physical Integrity

"Protecting from unauthorized access to the device."

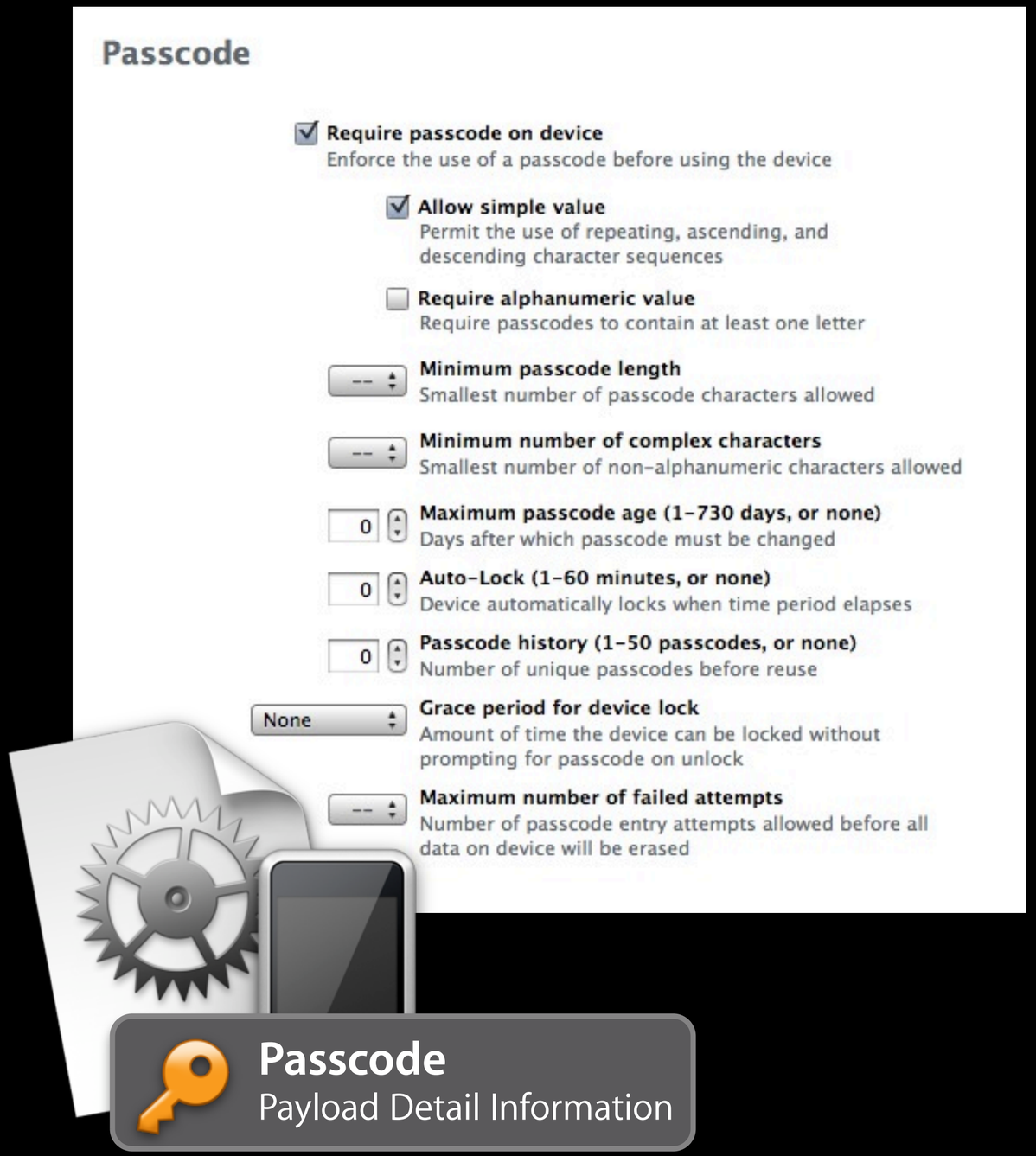
Passcode Protection

Settings > General > Passcode

- Default options
  - **Enforce** Manually
  - **Length** 4-digits fixed
  - **Simple PIN** 1111
  - **History** Last one used
  - **Device lock** 1 min.–4 hrs.
  - **Max Failures** 10 attempts

iPCU 2.0 Policy Setup

Config passcode complexity



- iPhone configuration utility
  - Requires passcode on device
  - Do not allow simple value
  - Requires alphanumeric
  - Min. passcode length [1–16] **10–12**
  - Min. complex chars [1–4] **2–3**
  - Max. passcode age [1–730] **120**
  - Auto-Lock [1–60] **1–2**
  - Max. failed attempts [4–16] **3–6***
  - Grace period - lock [–4h] **None**

Passcode Protection

Adds passcode complexity

- **Exchange ActiveSync (EAS)**
  - EAS protocol 12.1
  - Enforced password on device
  - Minimum password length
  - Maximum failed password attempts
  - Require numbers/letters
  - Inactivity time in minutes
- **Exchange 2007 policies**
  - Allow/prohibit simple password
  - Password expiration
  - Password history
  - Policy refresh interval
  - Minimum complex characters
  - Require manual syncing while roaming

Restrictions—Local

Access protection

- iPhone OS v2.2
  - Apps/services
  - App Store/installation
  - Hardware component use
    - Camera
  - Explicit content
- Locked
  - Restrictions passcode

Restrictions—Local

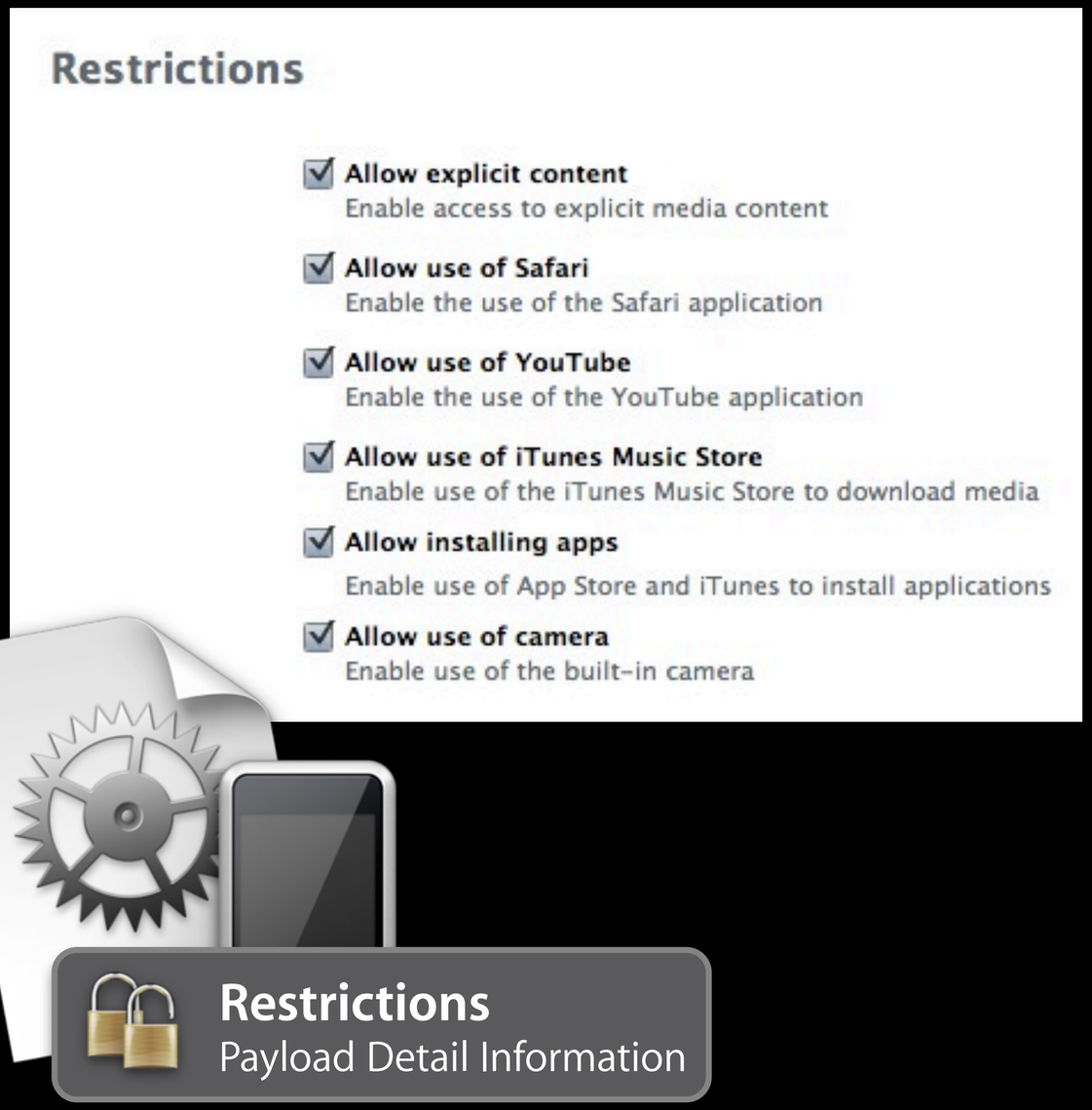
Access protection

- iPhone OS v3.0
  - Apps/services
  - App Store/installation
  - In-app purchase
  - Hardware component use
    - Camera, location
  - Explicit content
    - Movies, TV shows, apps
- Locked
  - Restrictions passcode

Restrictions—Policy

Enforce access restrictions

- iPhone OS v3
  - Content by ratings/explicit
  - Apps/services
  - App Store/installation
  - Hardware component use
    - Camera



Radio Interfaces

- Settings > Wi-Fi > off
  - Disable Wi-Fi (if not in use)
    - Disable ask to join networks
  - Disable Bluetooth (if not in use)
  - **OR**
- Settings > airplane mode > ON
  - Enable airplane mode
    - Turns radios off

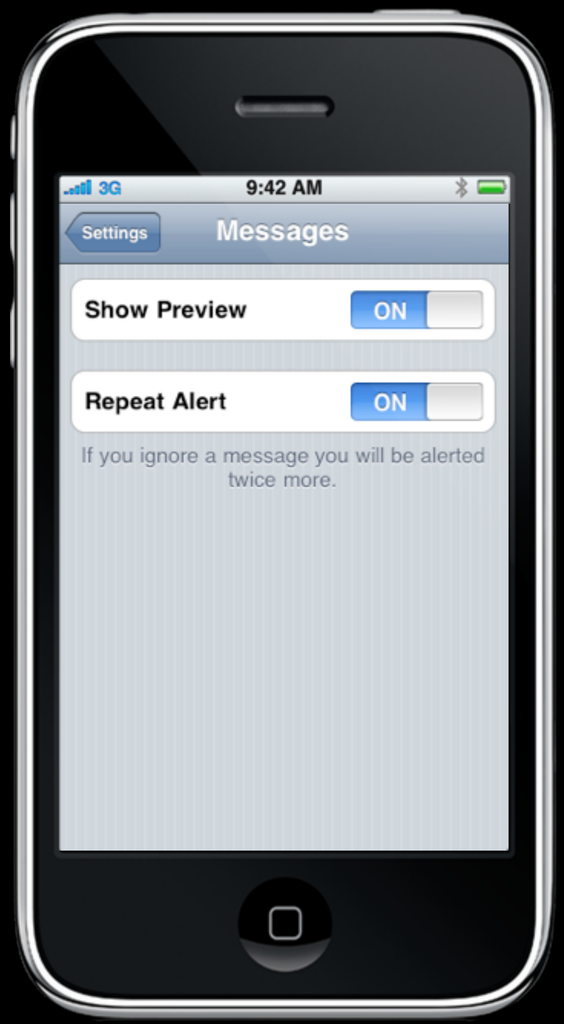
Recording

- Capturing audio
  - You can record audio
  - No current method to lockout microphone while not in phone application
- Secure environments
  - Consider deploying iPods

SIM Protection

Settings > Phone > SIM PIN

- Enable a **PIN** on the **SIM**
- Different than device passcode
- Second-level to cellular service
- SIM contents may be sensitive



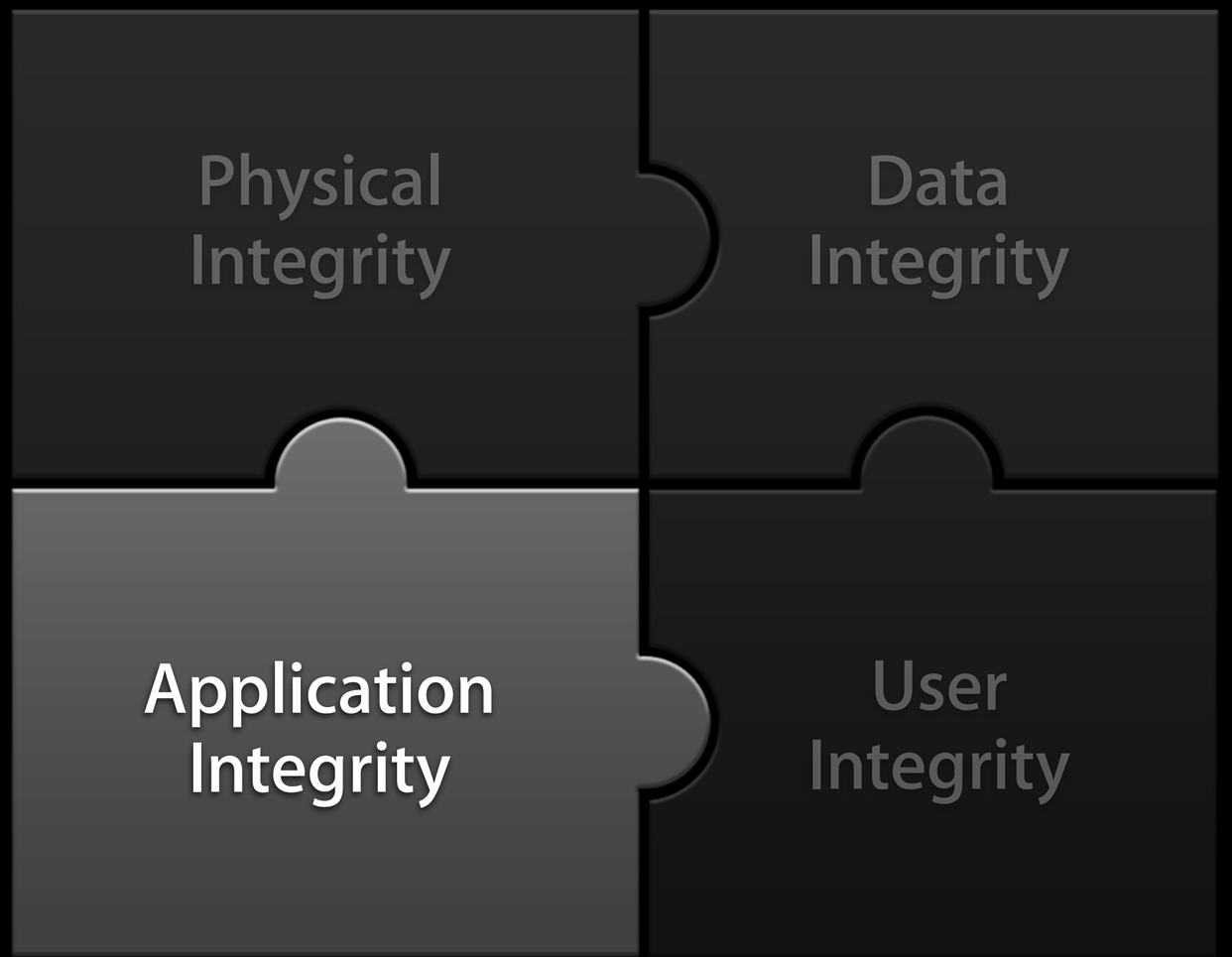
SMS Revelations

Settings > Messages > Preview

- Message display
  - Turn Show Preview off
  - Block potentially unwanted SMS messages appearing on screen
  - You cannot control what others say in their messages

Maintaining Integrity

A closer look at integrity



Application Integrity

Ensuring protection of applications and their services

Michael Brouwer
iPhone Security Architect

Application Integrity

"Protecting from modification through verification and trust."

Application Integrity

- Technology
  - Code signing
  - Sandboxing
- Distribution
  - Getting IT applications to your users

Code Signing

Verifying integrity of an application

- What it is used for
  - Ensure application has not been modified
  - Prevent the application from being modified after installation

- What it is used for
  - Cannot prevent an application from misbehaving
  - Does not protect **data** or communication
  - Does not ensure you are the authorized **user** to access corporate data

Trusting Applications

App Store applications

- Developed by a third party and signed by Apple
- Trusted by every device in the world

Trusting Applications

Your company applications

- Developed in-house and signed with your developer identity
- Trusted by the devices you control via provisioning profiles

Provisioning Profiles

Trusting additional applications

- Instructs a device to trust applications signed with your identity
- Restricted to a set of devices you select
- Signed by Apple, obtained through developer portal
- Allows you to control
  - Which in-house applications run in your organization
  - Which devices can run the applications

Benefits of Code Signing

- What does it help with?
  - Limits sources of rogue code
  - Raises the bar for code injection exploits
- What doesn’t it help with?
  - Social attacks
  - Correctness of code
  - Data-driven attacks

Sandboxing

Isolating applications from each other

- What it is
  - Mac OS X seatbelt technology that limits access based on the principle of least privilege
- What it is used for
  - Contrains access to only authorized resources
  - Preventing access to unauthorized resources
    - Prevents one app from accessing another app's data

Distributing Your Applications

Multiple ways to do it

- Both the provisioning profile and application must be installed
- You can use iTunes or iPhone Configuration Utility (iPCU)
- iTunes will automatically push both from known locations

Distributing with iTunes

Mac OS X

- Pushing the provisioning profiles(s)
  - Auto-installed by iTunes from
    - ~/Library/MobileDevice/Provisioning Profiles/
    - /Library/MobileDevice/Provisioning Profiles/
    - Path specified by the **ProvisioningProfilesPath** key in ~/Library/Preferences/com.apple.itunes
- Pushing the applications
  - Distribute to users, they drop into iTunes

Distributing with iTunes

Windows

- Pushing the provisioning profile(s)
  - Auto-installed by iTunes from
    - C:\Documents and Settings**username**\Application Data\Apple Computer \MobileDevice\Provisioning Profiles
    - C:\Documents and Settings**All Users**\Application Data\Apple Computer \MobileDevice\Provisioning Profiles
    - Path specified in the **HKCU** or **HKLM** by the Provisioning ProfilesPath registry key SOFTWARE\Apple Computer, Inc\iTunes
- Pushing the applications
  - Distribute to users, they drop into iTunes

Demo

Enterprise applications in action

Michael Brouwer
iPhone Security Architect

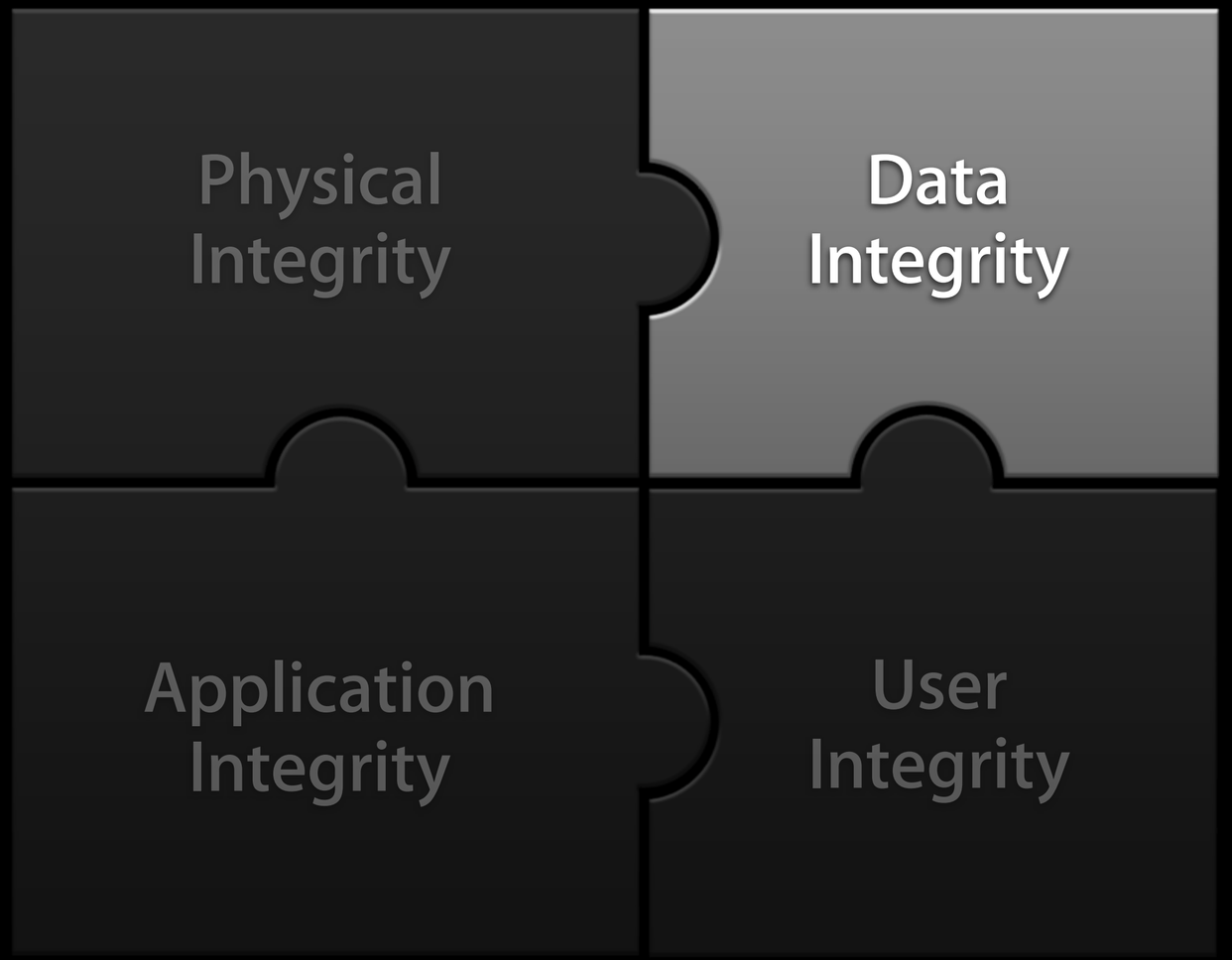
Installation on iPhone

Putting the enterprise application on the iPhone

- Provisioning profiles
- Automatically installed from predefined locations when syncing
- Can distribute .mobileprovision file for user to drop on iTunes app
- User manually installs applications via iTunes

Maintaining Integrity

A closer look at integrity



Data Integrity

Ensuring protection of enterprise data

Data Integrity

"Protecting from the modification or disclosure of data."

Data Integrity

- Certificate-based trust (X.509)
- Encrypted backups
- Data at rest on the iPhone
- Distribution
  - Getting IT applications to your users

Root Certificate Considerations

Pre-established trust

- iPhone OS
  - Trusts the same root certificates as Mac OS X
    - http://support.apple.com/kb/HT2185

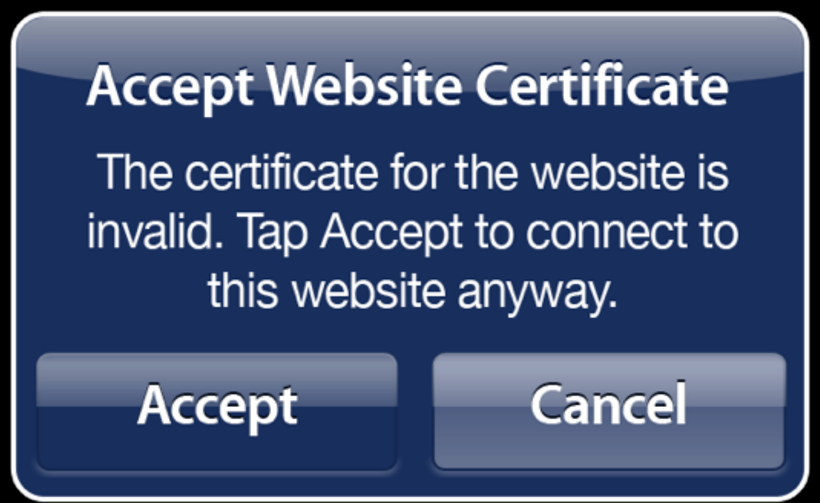
- New anchors can be added to the system via
  - Configuration profiles (.mobileconfig)
  - Email attachment (.cer, .crt, .der)
  - Downloading via Safari (application/x-x509-ca-cert)

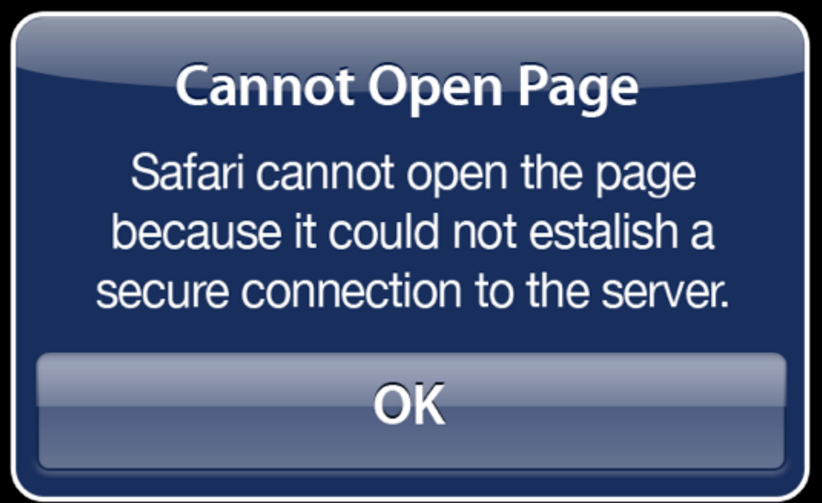
iPhone Server Certificate Validation

Server certificate must validate

- Your server ?
  - Add the necessary certificate(s) to the iPhone Configuration Profile

- External server ?
  - Should never connect





Demo

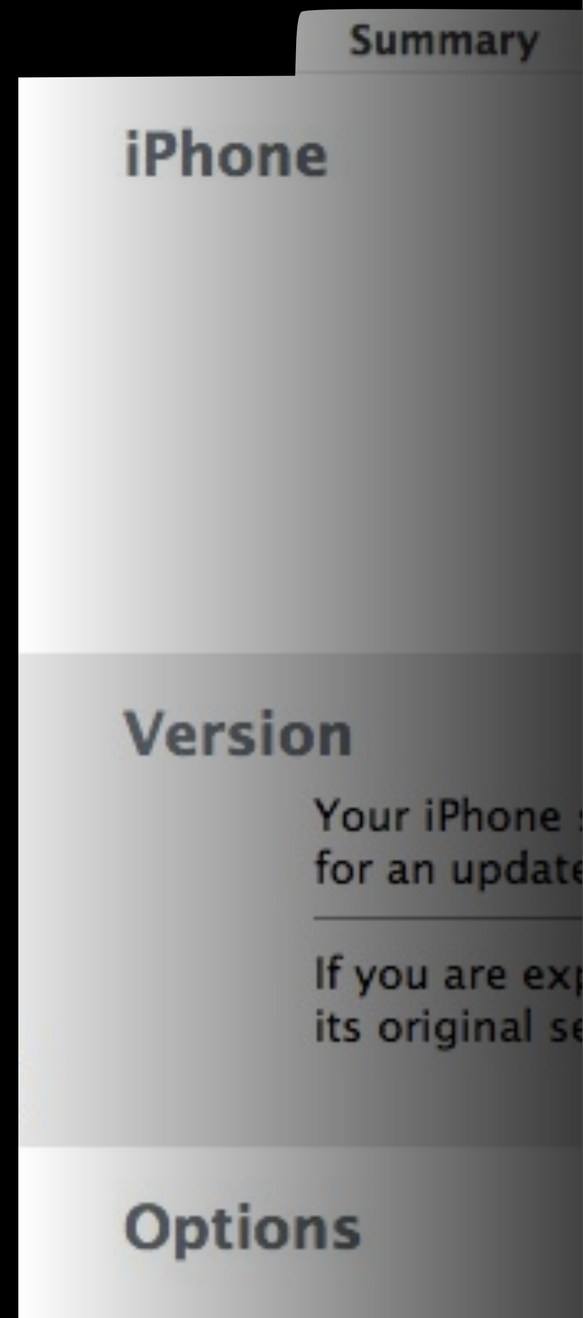
Extending trust

Mitch Adler
iPhone Security Engineer

Data at Rest on Computer

Protecting from disclosure on your computer

- iPhone backups are managed by iTunes
- Backups can now be encrypted



Data at Rest

Protecting from disclosure on your computer

- Stored on the computer used for syncing

```
~/Library/Application Support/MobileSync/Backup/<UDID>/
```

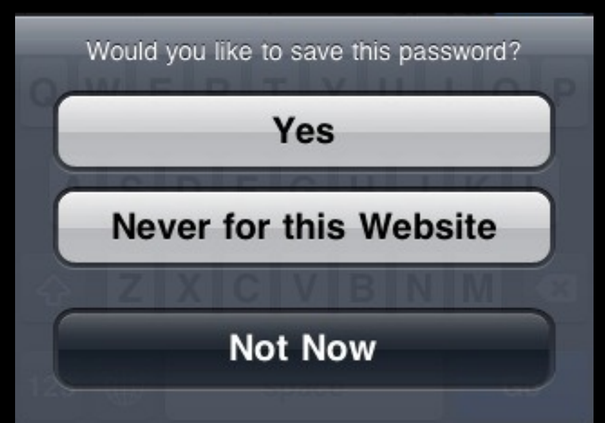
```
-rw-r--r-- <user> staff <size> <date> <obj_id>.mddata
-rw-r--r-- <user> staff <size> <date> <obj_id>.mdinfo
.....
-rw-r--r-- <user> staff <size> <date> Info.plist
-rw-r--r-- <user> staff <size> <date> Manifest.plist
-rw-r--r-- <user> staff <size> <date> Status.plist
```

Data at Rest on the iPhone

Protecting from disclosure

- Keeping sensitive data on corporate servers
  - Only store nonsensitive data locally on device
  - Utilize TLS for temporary data access
    - Secures transmission of data and credentials
    - No data stored locally on device if lost or stolen

- Applications with self-encrypting data storage
  - All iPhone applications can encrypt their own data
  - All iPhone applications have their own Keychain



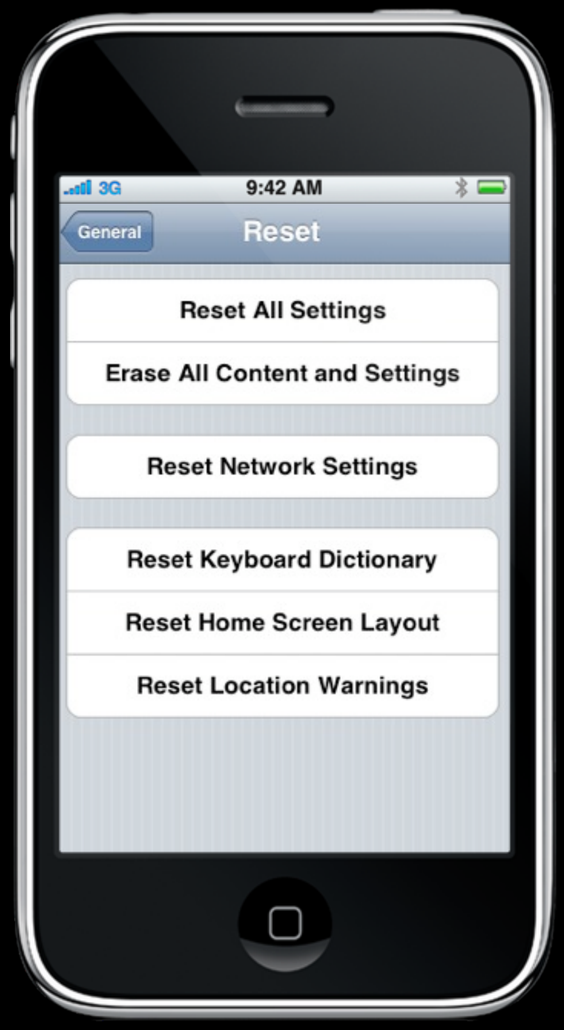
New for iPhone 3G S

Protecting from disclosure

- Hardware encryption of all user data
  - AES-256
- Instantaneous remote wipe

Restore to Redeploy

Settings > General > Reset

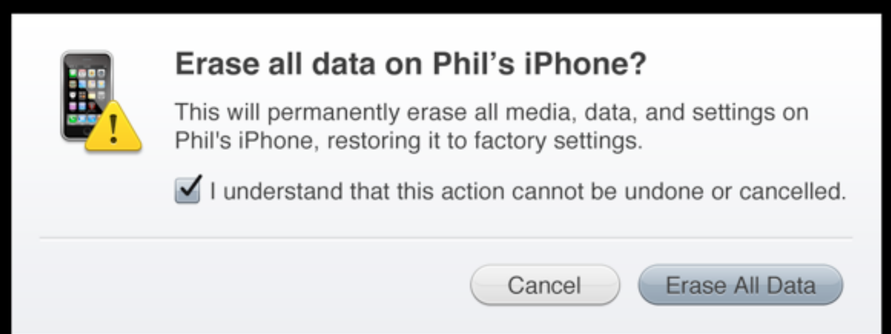


- Local wipe
  - Wipe all content and settings
    - Takes ~ 1 hour per 8GB pre-3G S
    - Be sure to plug into power
    - If battery runs out, will continue on powerup

Restore to Redeploy

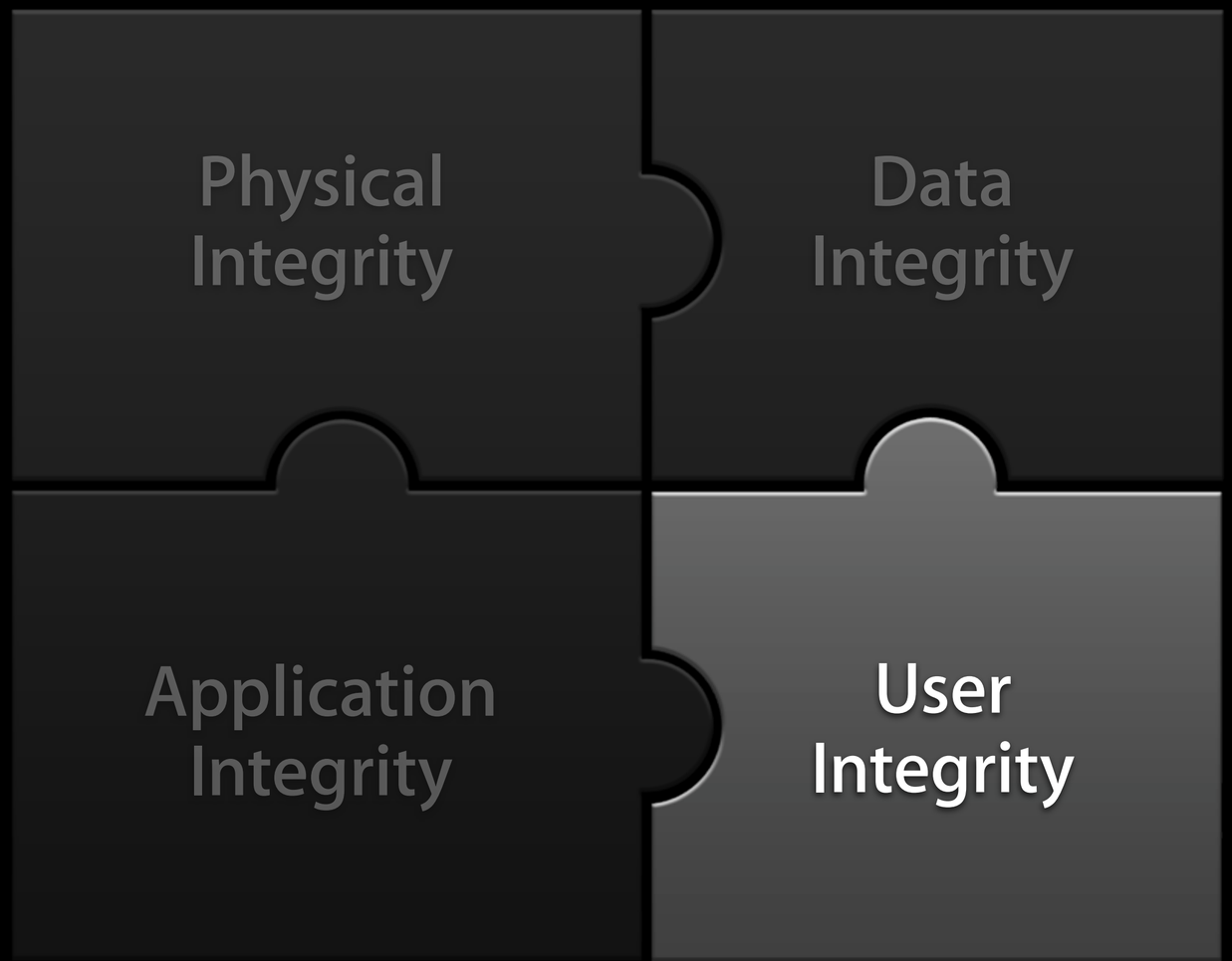
Remote wipe

- Exchange Server **2007**
  - Exchange Management Console
  - Outlook Web Access
  - Exchange ActiveSync Mobile Administration Web Tool
- Exchange Server **2003**
  - Exchange ActiveSync Mobile Administration Web Tool
- MobileMe
  - One-to-one registration of phones



Maintaining Integrity

A closer look at integrity



User Integrity

Ensuring authorized user is who they claim they are

Mitch Adler
iPhone Security Engineer

User Integrity

"Ensuring users get exactly the access they should have."

What Problems Are We Trying to Solve?

- User credentials
  - Authoritatively establish who the user is
  - Protect the user's credentials on the device
- Enterprise IT
  - Protect services from unauthorized access
  - Support industry standard verification

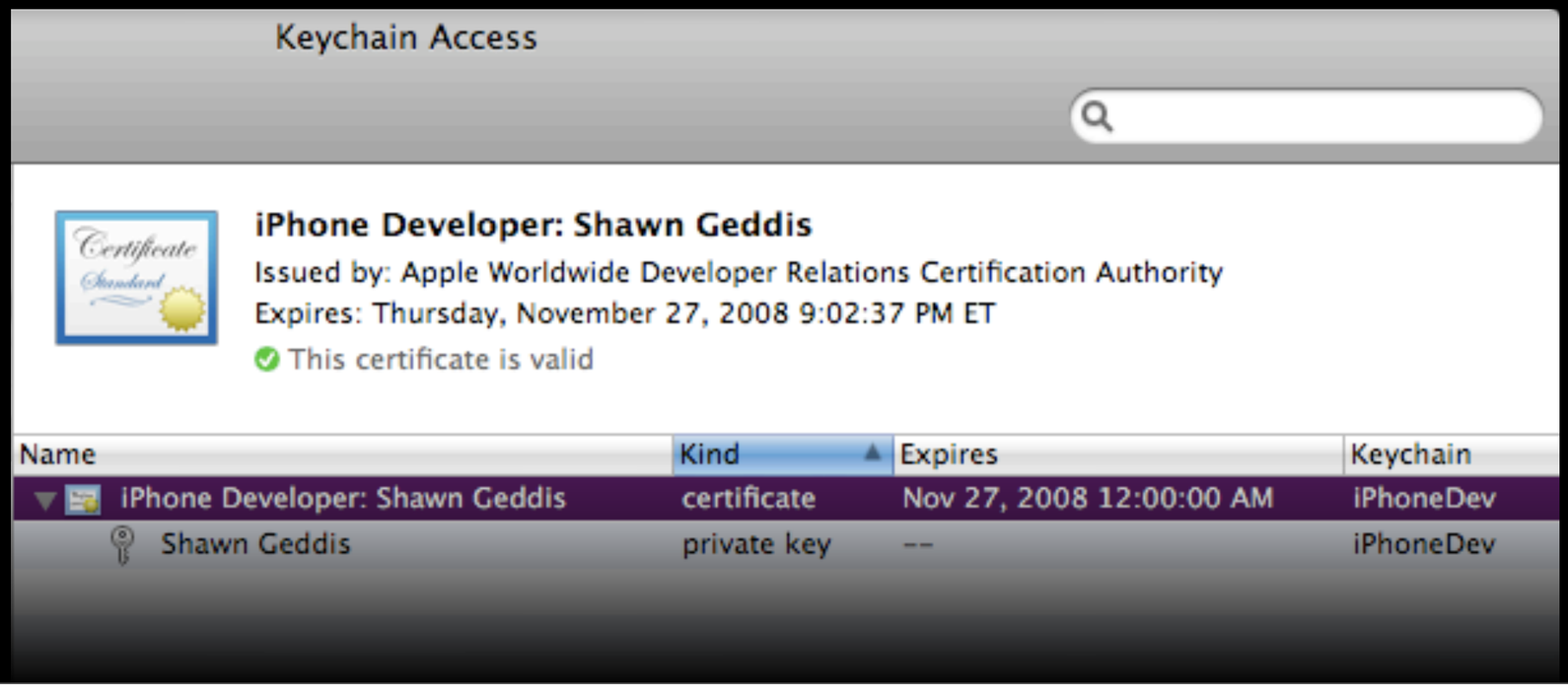
Forms of Credentials

- Passwords — A shared secret between mulitple parties
  - Mail, calendars
- One-time passwords — Requires user entry every time it's used
  - VPN, 802.1x
- X.509 digital identity — Requires significant infrastructure
  - VPN, 802.1x, Safari

Identity

X.509 certificate and private key

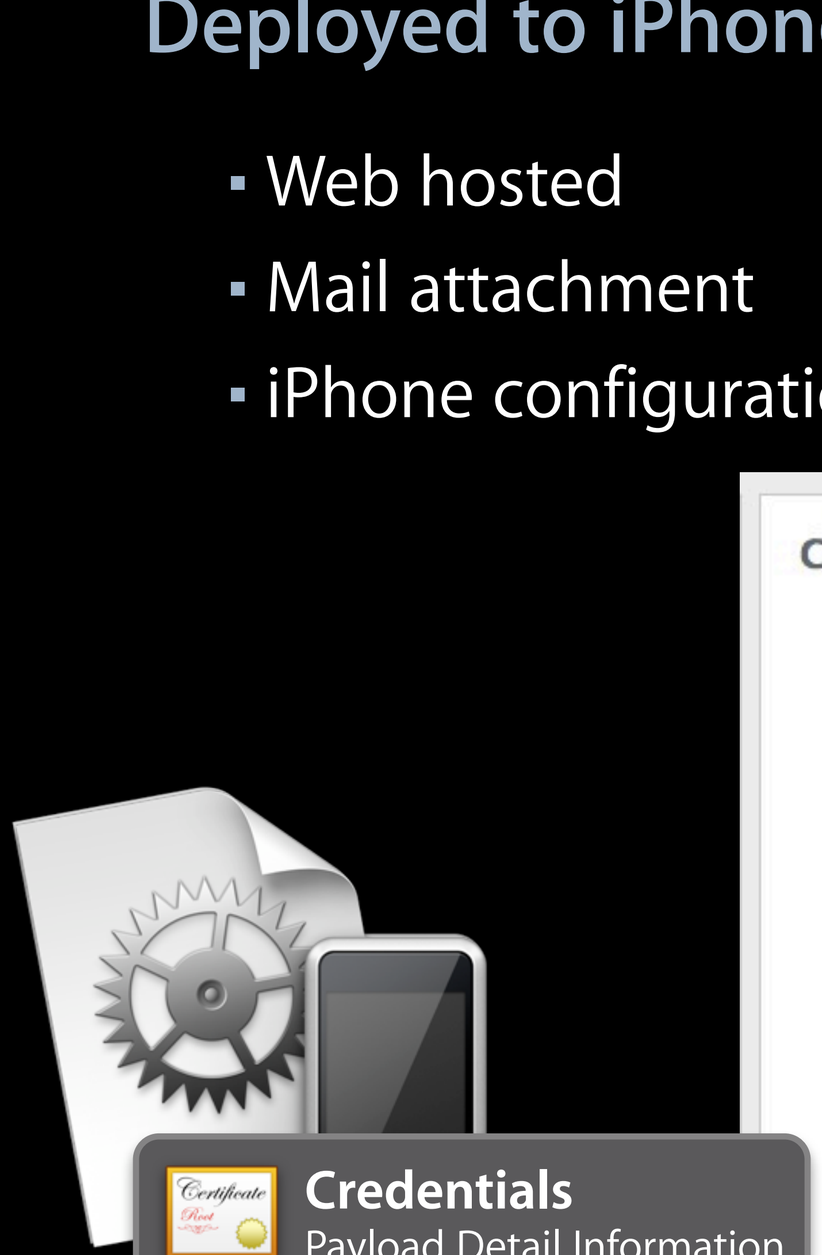
- Certificate
  - Identifies the key holder and permitted usage
- Private key
  - Secret held to prove identity

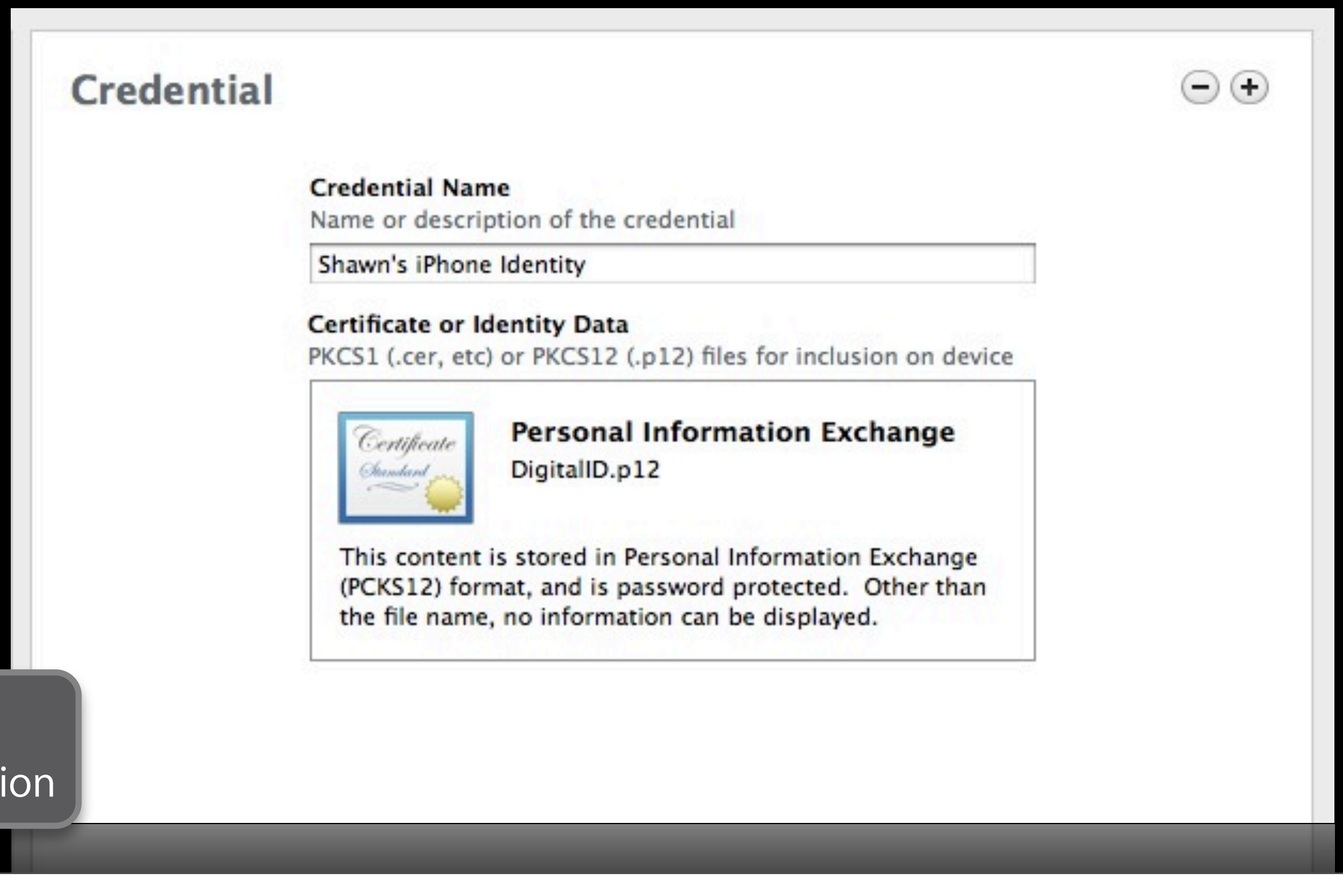


Deploying Your Identity

Deployed to iPhone

- Web hosted
- Mail attachment
- iPhone configuration utility

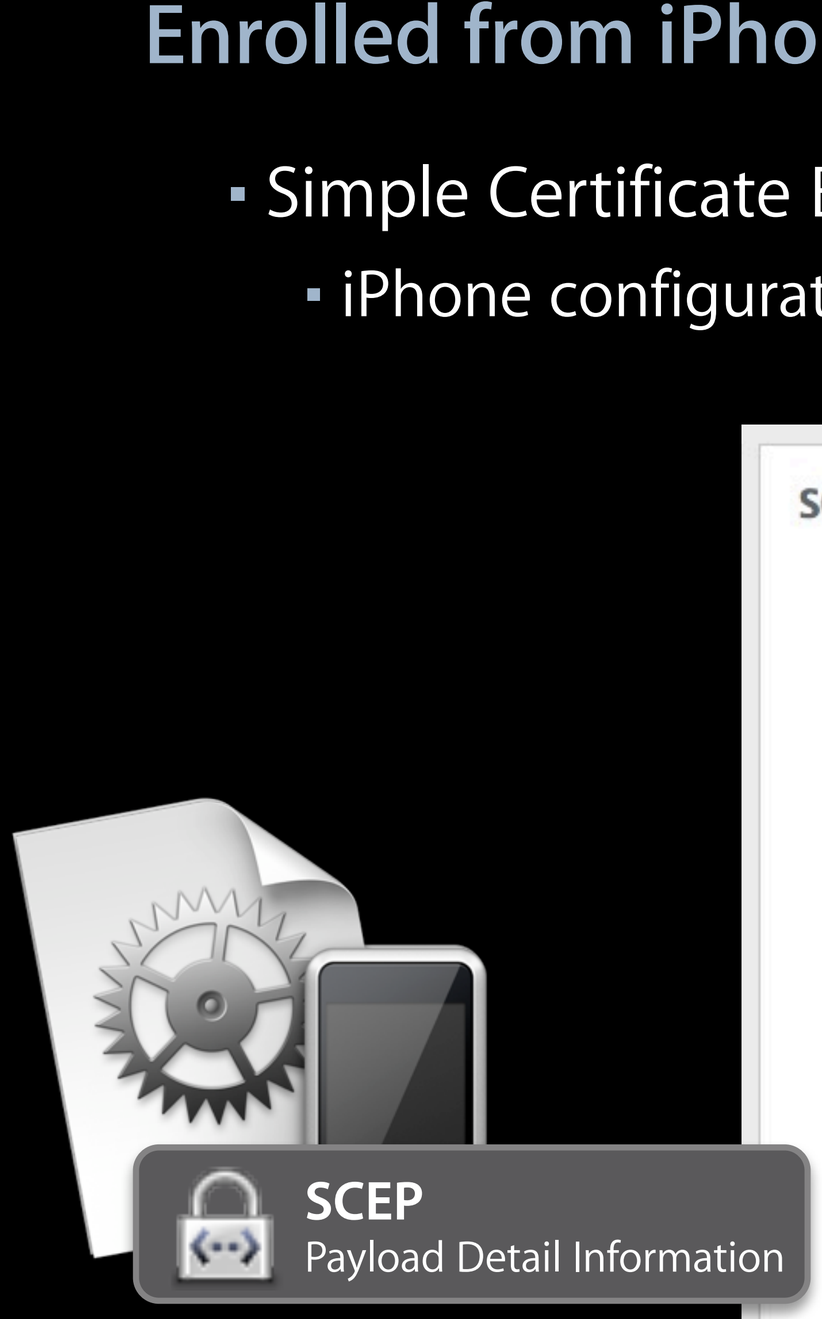


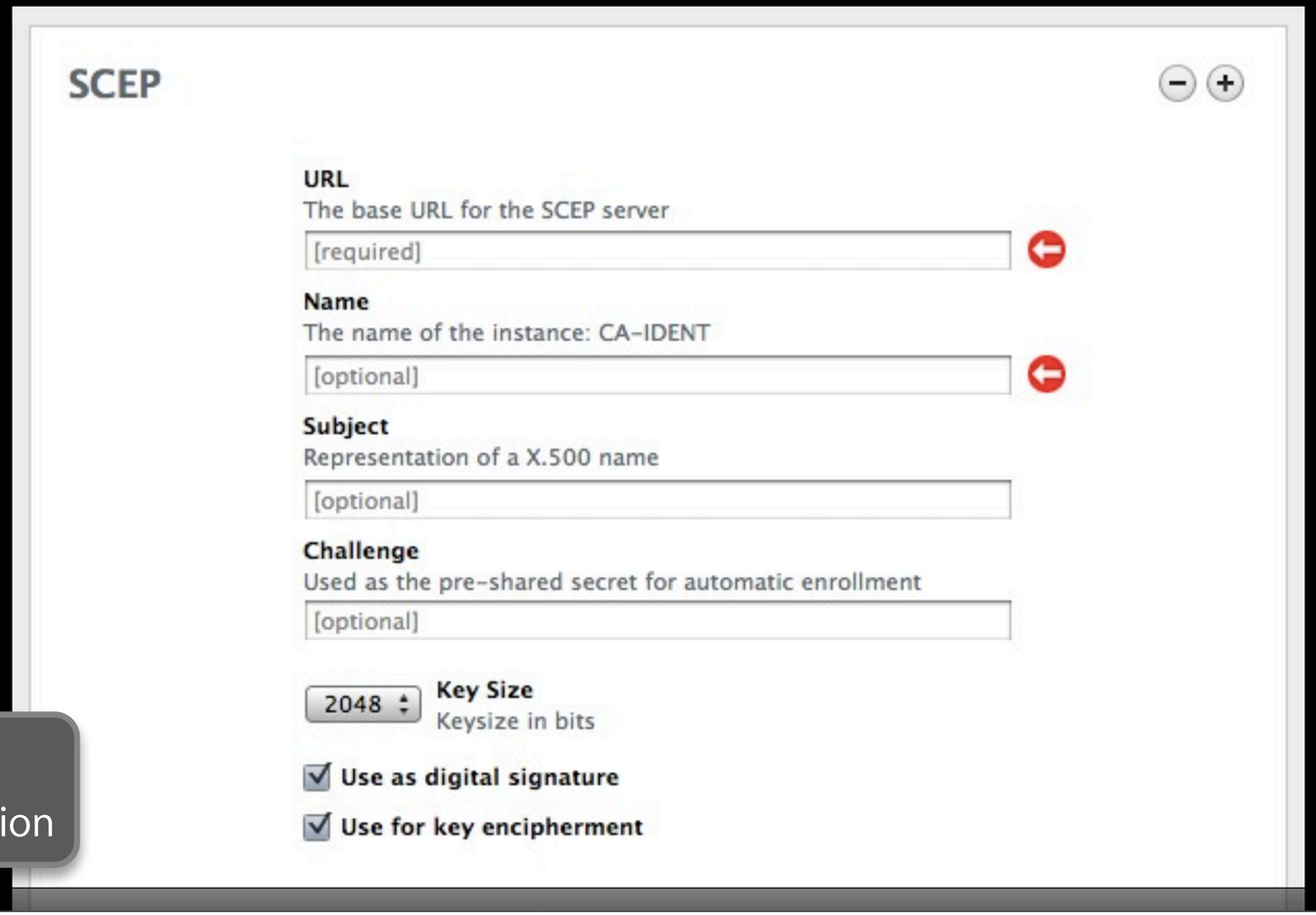


Deploying Your Identity

Enrolled from iPhone

- Simple Certificate Enrollment Protocol (SCEP)
  - iPhone configuration creation and deployment session

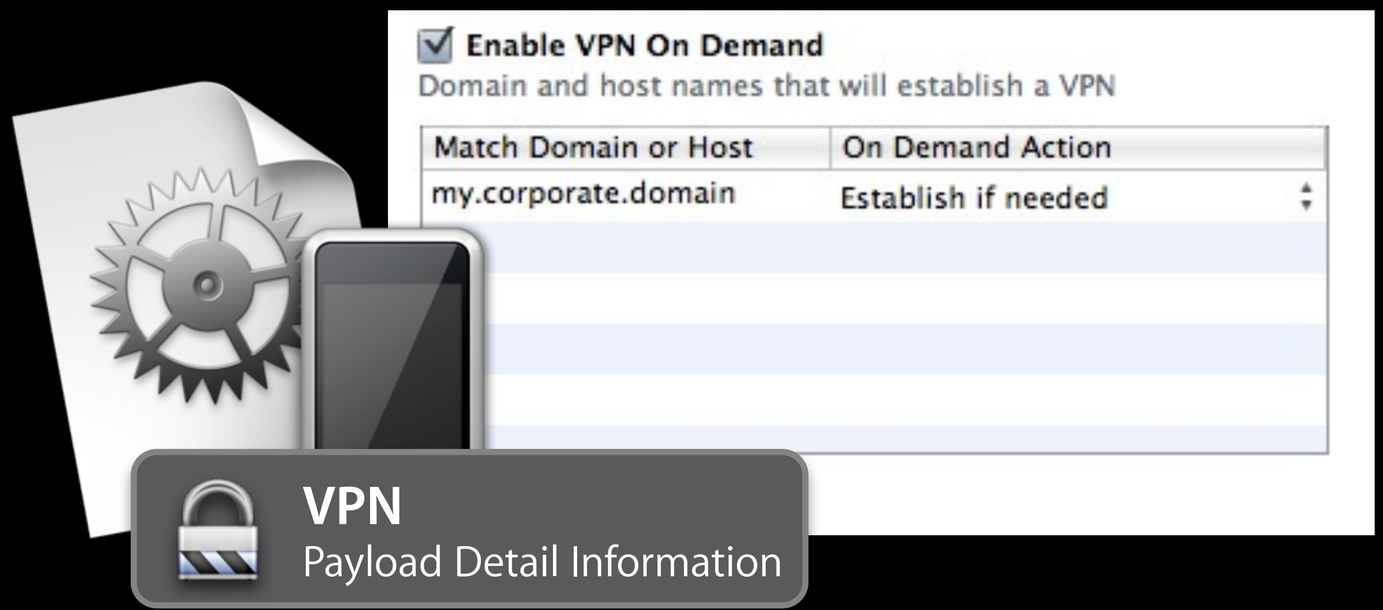




Example of Identity Use

iPhone using X.509 identities

- Machine identity
  - VPN
    - IPSec (Cisco)
      - VPN on-demand



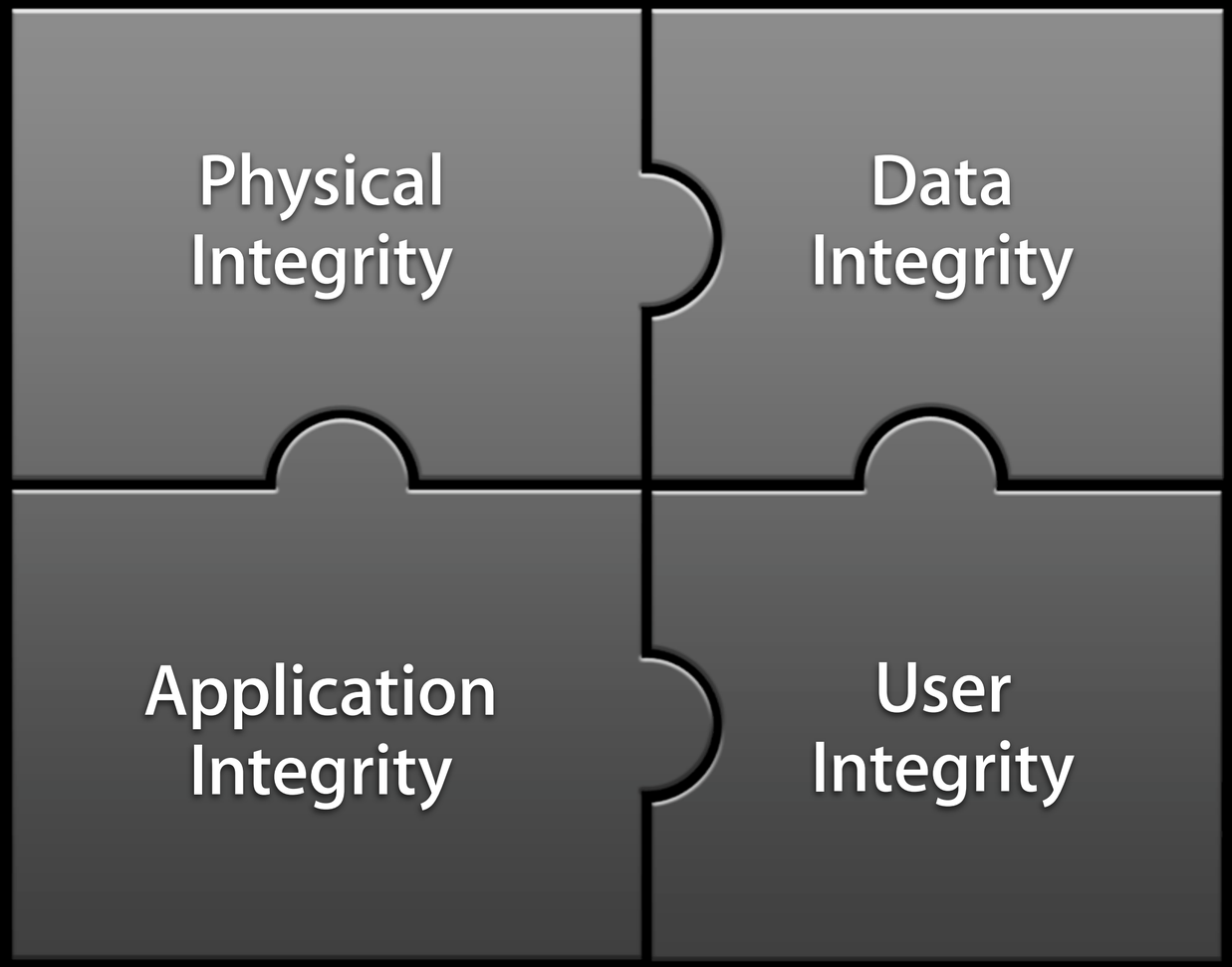
Custom User Integrity

Other authentication methods

- External authentication
  - Two-factor authentication

Maintaining Integrity

A closer look at integrity



Policy Deployment

Profile deployment best practices

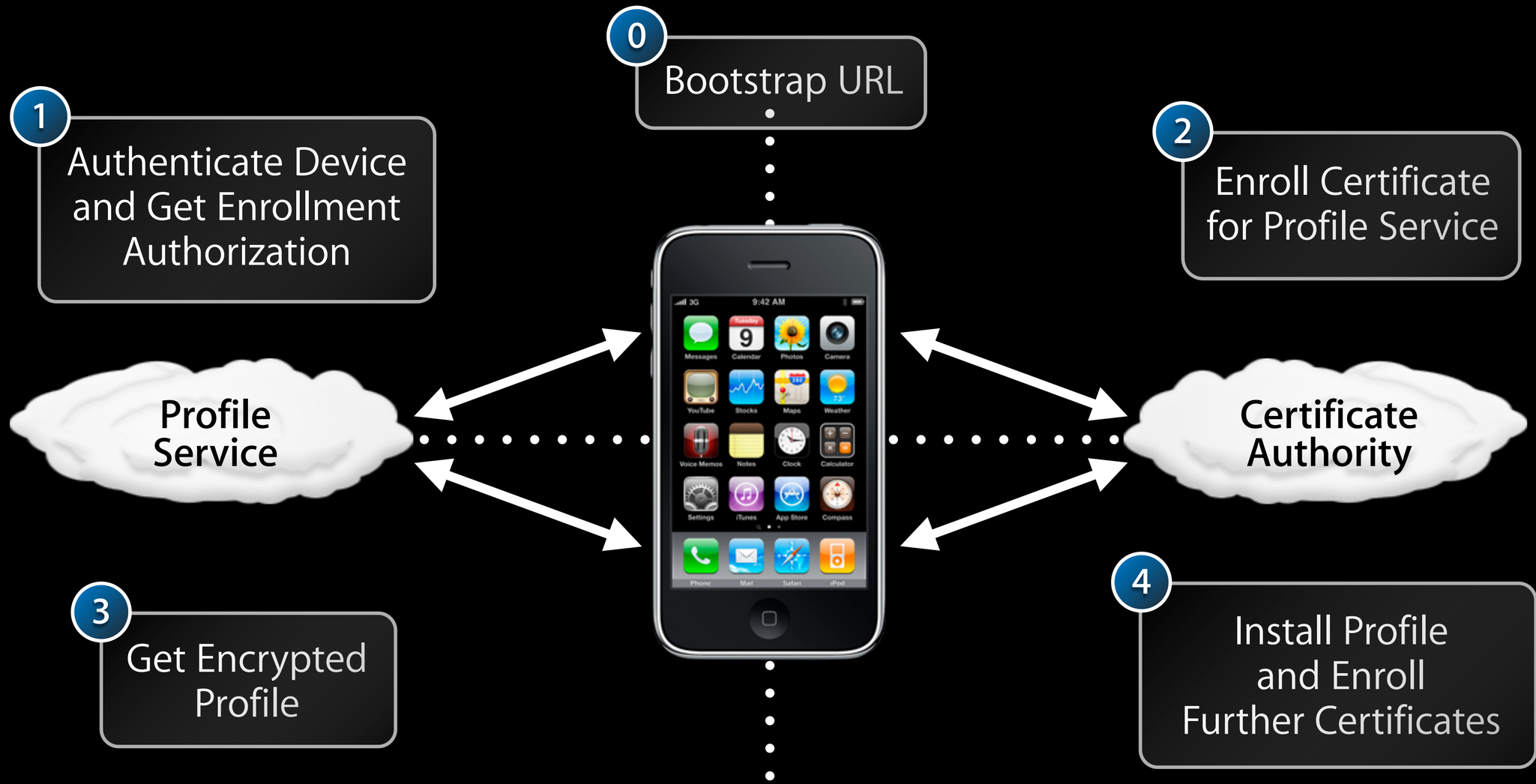
Profile Deployment Best Practices

Offering the carrot and stick

1. Profile for public credentials (e.g., Anchors CAs)
2. Another profile/set of profiles for user settings
   - iPhone will prompt for information omitted in profile such as user name, user password

OTA Enrollment

Simple Certificate Enrollment Protocol (SCEP)



Summary

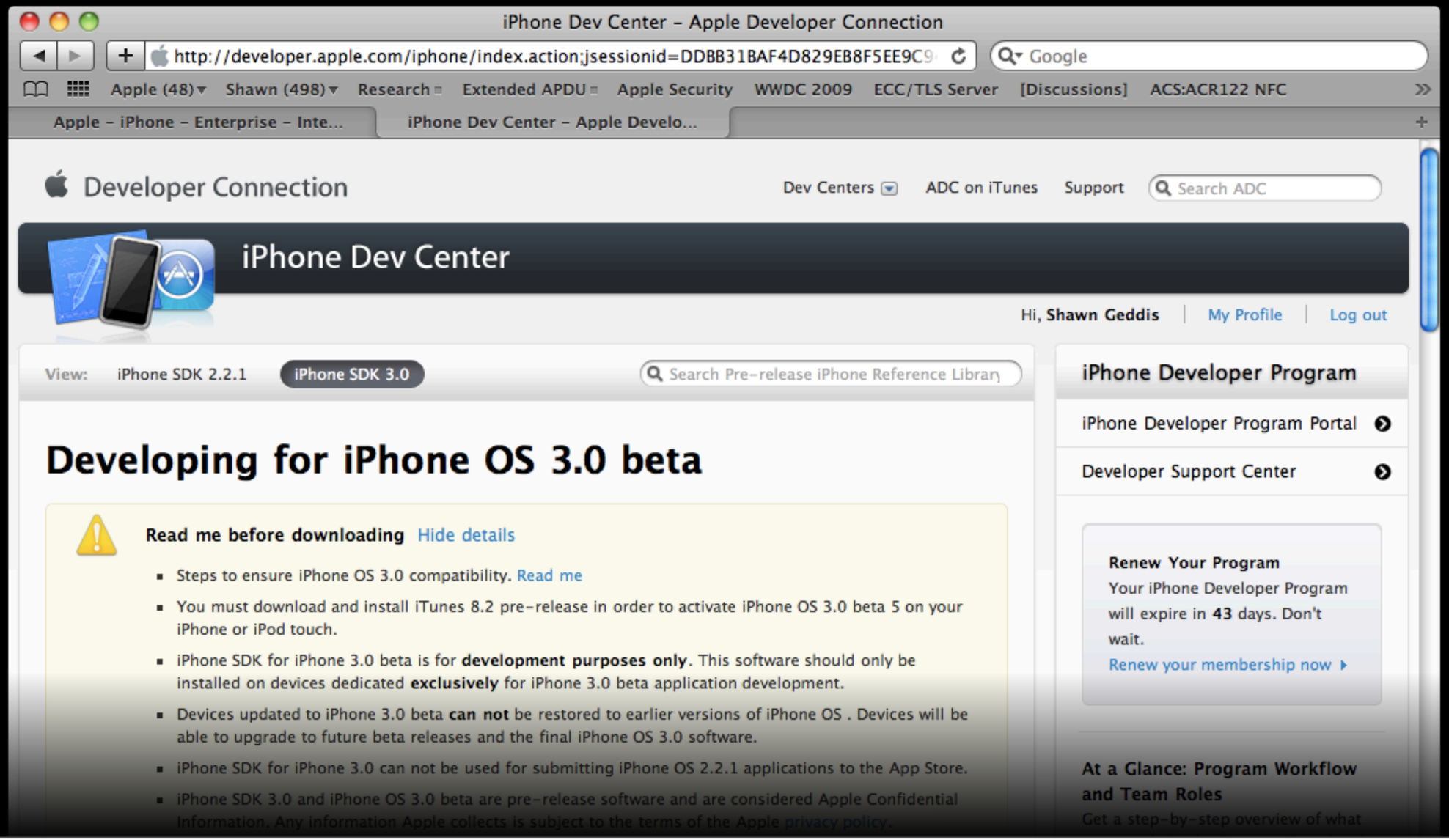
- iPhone OS has built-in proactive security technology for defense
- Balance the needs and ease of use against risks
- iPhone OS policies can be securely distributed to the device
- iPhone OS can be tailored to your corporate policies

Where to Go for More Guidance

Continuing the guidance legacy with iPhone

iPhone in the Enterprise Resources

General guidance on deploying iPhone in the enterprise



Collaboration and Validation on Best Practices

Vetting the settings with the experts

iPhone Security Guidance

U.S. Federal Government efforts

- iPhone guidance is already under development
- Development using policies for enterprise environment
- Federal Desktop Core Configuration (FDCC) will be produced
  - Interim security guidance for standalone iPhones can be recommended based on standard security principles

More Information

iPhone in Enterprise
http://www.apple.com/iphone/enterprise/

iPhone Dev Center
Technical iPhone Developer Resources
http://developer.apple.com/iphone/

Apple—Security Configuration Guides
Security Guidance for Mac OS X, Server, and iPhone
http://www.apple.com/support/security/guides/

NSA—Security Configuration Guides
Security Guidance for most platforms
http://www.nsa.gov/ia/guidance/security_configuration_guides/index.shtml

Apple Training and Certification
http://training.apple.com

Related Sessions

Creating Secure iPhone and Mac OS X Applications	Russian Hill Tuesday 5:00PM
iPhone Configuration Creation and Deployment	Pacific Heights Thursday 3:30PM
Secure Access with 802.1X	Nob Hill Friday 2:00PM

Labs

iPhone OS Security	iPhone Lab D Thursday 5:00PM
iPhone Configuration Profiles Creation and Deployment	Information Technologies Lab Thursday 5:00PM

Q&A

WWDC Session Survey

You can rate your sessions on the WWDC Attendee Site.

Survey forms are located on each session description page at:

developer.apple.com/wwdc/attendee

WWDC09